UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

ABDULKADIR NUR,

Plaintiff,

Case No.

v.

UNKNOWN CBP OFFICERS, in their individual capacity,

CHRIS MAGNUS, Commissioner, U.S. Customs and Border Protection; in his official capacity, only, and

CHRISTOPHER WRAY, Director, Federal Bureau of Investigations; in his official capacity, only,

Defendants.

COMPLAINT

Plaintiff Abdulkadir Nur, for himself and through his attorneys, CAIR Legal Defense Fund ("CAIR-LDF"), states as follows:

Introduction

1. Abdulkadir Nur is a 69-year-old American citizen living in northern Virginia. He is Muslim and from Somalia, having been naturalized more than 15 years ago. And yet, every single time he lands at Dulles International Airport or anywhere else from overseas, CBP officers illegally seize any phone or laptop with him.

2. These CBP officers do so as part of a brazen, government-wide program aimed at surveilling Mr. Nur and the Muslim community he belongs to.

3. Mr. Nur has never been charged, let alone, convicted of a crime. He is not

under investigation. And CBP officers are seizing and searching his electronic devices, not as part of their duties to protect our borders, but instead with the institutional goal of adding data unlawfully taken from his devices to the vats of information the federal government compiles on innocent American travelers like Mr. Nur.

4. Beyond the federal government's institutional goal to gobble up as much information as possible, the specific reason CBP officers illegally took five of Mr. Nur's phones and laptops at Dulles International Airport in the last four months is as simple as it gets: their computers told them to.

5. More than a decade ago, an FBI official imposed on Mr. Nur a status that identifies him as worthy of permanent suspicion. That FBI official did so in accordance with secret standards, secret processes, and using secret evidence.

6. Since imposing that status on Mr. Nur, the FBI has disseminated that label to tens of thousands of entities all over the world—hospitals, universities, every law enforcement agency in the country, foreign governments, and for-profit corporations. The FBI also communicated Mr. Nur's status to the Unknown CBP Officers who seized and searched his electronics.

7. Since being assigned this status, each time Mr. Nur came back to his home in Virginia, these Unknown CBP Officers saw Mr. Nur's status and the annotations CBP and other federal agencies affixed to it and did what those conclusory labels told them to do. They took the electronic devices of a 69-year old American citizen coming to the United States to see his children.

8. The Constitution demands more than this. The automated decision making that Defendants have used to justify the seizure of Mr. Nur's electronic devices and those of

countless others throughout the Muslim community falls short of what this Court must expect of the federal government.

Parties

9. Plaintiff Abdulkadir Nur is a United States Citizen of Somali descent and a Muslim living in northern Virginia. Venue is proper because a substantial part of the events or omissions giving rise to his claims occurred within this district which is where the FBI official who assigned him a watchlist status did so. Upon information and belief, Defendant FBI made the decision to place Plaintiff Nur in the TSDB.

10. Defendant Magnus is Commissioner of the United States Customs and Border Protection ("CBP") of the DHS. CBP is a regular agency attendee of the Watchlisting Advisory Council ("WAC"), a government agency that promulgates decisions regarding all policies, procedures, practices and instructions pertaining to the federal terrorist watchlist, including, but not limited to: (1) watchlist nomination and removal procedures; (2) specific criteria used to nominate persons to the Terrorist Screening Database ("TSDB"); (3) redress procedures; and (4) vetting of information used to nominate persons to the TSDB. CBP represents DHS at WAC meetings. Because the WAC operates by consensus, CBP has both decision-making authority and veto power over all decisions made by the WAC. Upon information and belief, CBP acts as a front-line agency that utilizes the TSDB to screen individuals against the TSDB, including the Plaintiff and other similarly situated Americans, to seize and search Plaintiff' electronic devices and the electronic devices of similarly situated Americans. Moreover, upon information and belief, CBP nominated the Plaintiff, and continues to nominate other similarly situated American citizens, permanent residents, and foreign nationals to the federal terrorist watchlist and assigns an "armed and dangerous" annotation to innocent people like PlaintiffDefendant Magnus is being sued in his official capacity, only.

11. The Unknown CBP Officers are employees of the CBP who carried out the searches and seizures on April 28, 2018, October 9, 2019, February 2020, June 30, 2020, August 15, 2020, September 2021, and January 25, 2022. On information and belief, the identity of these officers are known by the CBP.

Jurisdiction and Venue

12. Under U.S. Const. Art. III § 2, this Court has jurisdiction because the rights sought to be protected herein are secured by the United States Constitution.

13. Jurisdiction is proper pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, 5 U.S.C. § 706, the United States Constitution, and federal common law.

14. This Court has authority to grant the declaratory relief requested herein pursuant to the Declaratory Judgment Act, 28 U.S.C. § § 2201-02, because the action presents an actual case or controversy within the Court's jurisdiction, and pursuant to the general, legal, and equitable powers of this Court.

15. Nothing in 49 U.S. § 46110 eliminates that jurisdiction. See, e.g., *Mohamed v. Holder*, No. 11-1924, 2013 U.S. App. LEXIS 26340, at *5-6 (4th Cir. May 28, 2013); *Ege v. United States Dep't of Homeland Sec.*, 784 F.3d 791, 796 (D.C. Cir. 2015); Latif v. Holder, 686 F.3d 1122, 1128-29 (9th Cir. 2012); *Wilwal v. Nielsen*, 346 F. Supp. 3d 1290, 1304 (D. Minn. 2018).

16. A substantial part of the unlawful acts alleged herein were committed within the jurisdiction of the United States District Court for the Eastern District of Virginia.

17. Venue is proper under 42 U.S.C. § 1391(e)(1) because at least one of the Plaintiff resides in this district; because Defendants are officers or employees of agencies of the United States sued in their official capacities; because Defendants regularly conduct business

in the State of Virginia; because a substantial part of the events or omissions giving rise to Plaintiff' claims occurred within this district; and because the action involves no real property.

Factual Background

The Federal Government's Expansive TSDB Inclusion Standards Capture Broad Categories of Innocent Travelers

18. In September 2003, without the authorization of Congress and relying expressly on Executive Order HSPD-6, Attorney General John Ashcroft established the Terrorist Screening Center ("TSC") as a division of the FBI focused on building what the federal officials running the program call their "watchlist enterpirse." The TSC develops and maintains the federal government's consolidated Terrorism Screening Database ("TSDB" or "federal terrorist watchlist"). TSC's watchlist, and the tens of thousands of agreements the FBI maintains to compel agencies, companies, and organizations of all kinds to check its lists, is how the federal government is able to impose a disfavored status on Mr. Nur and more than one million other people.

19. Two government entities are primarily responsible for "nominating" individuals for inclusion in the terrorist watchlist—NCTC and FBI. The NCTC, which is managed by the Office of the Director of National Intelligence, relies on information from other federal departments and agencies when including alleged known or suspected international terrorists in its Terrorist Identities Datamart Environment ("TIDE") database. The NCTC reviews TIDE entries and recommends specific entries to the TSC for inclusion in the watchlist. The FBI, in turn, nominates to the watchlist individuals with what it characterizes as suspected ties to domestic terrorism.

20. CBP also nominates individuals for inclusion in the terrorist watchlist.

21. CBP employs risk-based targeting rules to single out travelers at ports of entry for secondary inspection, detention, investigation and deportation. Upon information and belief, CBP utilizes the results of high-risk targeting rules and resulting inspections and investigation as a factual predicate for nominating individuals to the TSDB.

22. All nominations to the TSDB must be approved and implemented by the TSC. The TSC makes the final decision on whether a nominated individual meets the minimum requirements for inclusion into the watchlist as a known or suspected terrorist. TSC also decides which screening systems will receive information about that individual.

23. The federal government publicly states that to be included in the TSDB, an individual must be reasonably suspected of being a known or suspected terrorist. More specifically, a government nominator, including CBP, "must rely upon articulable intelligence or information which, based on the totality of the circumstances and taken together with rational inferences from those facts, creates a reasonable suspicion that the individual is engaged, has been engaged, or intends to engage, in conduct constituting in preparation for, in aid or in furtherance of, or related to, terrorism and/or terrorist activities."

24. The "totality of the circumstances" analysis for TSDB inclusion may include assessment of an individual's race, ethnicity, country of origin, religion, religious practices, languages spoken, family, associations, travel history, social media history, and other activities protected by the First Amendment, Fifth Amendment, Fourteenth Amendment, and U.S. Constitution.

25. Former Director of the Terrorism Screening Center Timothy Healy testified that in evaluating whether an individual meets the criteria for inclusion on the consolidated watchlist, the TSC determines whether the nominated individual is "reasonably suspected" of having possible links to terrorism. According to the TSC, "reasonable suspicion requires

articulable facts which, taken together with rational inferences, reasonably warrant the determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in and of or related to terrorism and terrorist activities."

26. The federal government has provided only limited information about and otherwise not stated publicly what standards or criteria they use to assign and annotate a status.

27. The standards for watchlist inclusion do not evince even internal logic. The Watchlisting Guidance[1] defines a "suspected terrorist" as an "individual who is reasonably suspected to be, or have been, engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and terrorist activities based on articulable and reasonable suspicion."

28. In other words, pursuant to official federal government policy, Americans and other individuals are placed on the federal terrorist watchlist based upon a "reasonable suspicion" that they are "reasonably suspected" of nefarious activities. These standards fall far below the established "reasonable suspicion" and "probable cause" standards required for criminal investigation.

29. Individuals may also be added to the TSDB based on guilt-by-association as a basis for watchlist inclusion. For example, immediate relatives of listed persons can become TSDB listees without any derogatory information—other than the bonds of family. Likewise, they can be subjected to CBP rules-based 'terrorist' monitoring on the basis of family affiliation alone. Such annotations signals to screening agencies, officers, employers, and others that the immediate relative is a violent threat engaged in nefarious activities.

30. Individuals may be added to the TSDB for being a known associate—a friend, colleague, fellow community member, etc.—of a TSDB listed individual.

31. Even if an American citizen is acquitted of terrorism charges or those charges are otherwise dismissed, they can and routinely are added to the watchlist.

32. American citizens can be and are routinely added even if they are not the subject of a federal investigation.

33. Individuals can be added to the federal terrorist watchlist without any information regarding whether or not an intended target exists, and without any information about whether an individual poses a threat to commercial aviation or to a U.S. land border.

34. Individuals can be added to the federal terrorist watchlist without ever having been charged or convicted of any crime.

35. The FBI has conceded that because the federal terrorist watchlist "only includes identifiers of known or suspected terrorists, by itself [the FBI] is not aware of any instance where that identifying information alone prevented an act of terrorism."

36. CBP has also conceded that it has never publicly identified an act of terrorism that its use of TSDB information prevented.

37. Because of these loose standards and practices, the federal terrorist watchlist's rate of growth has dramatically increased. In fiscal 2009, there were 58,999 new additions to the watchlist. Over 1.1 million new names have been added to the watchlist since 2009. In fiscal 2016, for example, there were 176,014 new additions. These additions include thousands of U.S. citizens and lawful permanent residents.

38. More than 98% of the names nominated to the TSDB are accepted. In 2013, TSC accepted 98.96 percent of all nominations made. A 2007 GAO report found that TSC rejects only approximately one percent of all nominations to the watchlist.[1]

[1] *See* United States Government Accountability Office Report to Congressional Requesters entitled *Terrorist Watchlist Screening: Opportunities Exist to Enhance Management Oversight, Reduce*

39. Upon information and belief, in 2001, there were 16 people who the federal government systematically prevented from flying. By 2009, the number grew to approximately 3,400. By 2016, that number increased to approximately 81,000.

40. At a March 10, 2010, Senate Homeland Security Committee hearing, Russel E. Travers, Deputy Director of the National Counterterrorism Center, stated that "[t]he entire federal government is leaning very far forward on putting people on list," and that the watchlist is "getting bigger, and it will get even bigger."

41. The federal terrorist watchlist's and rules-based terror lists' inclusion standards are so permissive, pliable, and laden with discriminatory assessments of race, ethnicity, national origin, and religion, that they bear at best a fleetingly marginal connection to actual terrorist activities.

42. Based on the University of Maryland's Global Terrorism Database, a project funded in part by the Department of Homeland Security, there have been less than 250 terrorist acts inside the United States over the last decade. These terrorist acts were perpetrated by less than 250 persons.

43. Only one of these perpetrators was designated on the federal terrorist watchlist by the federal government prior to their criminal conduct. This single person designated on the federal terrorist watchlist, however, was removed from the federal terrorist watchlist prior to perpetrating the terrorist attack.

44. Upon information and belief, in order to designate a person on the federal terrorist watchlist, the federal government must first have information about that person. Because the federal government does not possess information on every person in the world,

---

Vulnerabilities in Agency Screening Processes, and Expand Use of the List, GAO-08-110, October 2007, at 22.

existing law enforcement and intelligence practices produce a subset of persons who the federal government can then screen against the federal terrorist watchlist's inclusion standards.

45. The precise size of this subset is unknown; however, a survey of law enforcement and intelligence practices indicates that the size of this subset is greater than 50 million people.

46. Upon information and belief, the practices that produce this subset exclude some persons who do pose a threat of terrorism and include innocent persons who do not pose a threat of terrorism.

47. Upon further information and belief, the federal government does not screen the entire subset of people known to it. Moreover, federal government does not make individual determinations as to whether each person about whom they have information should be placed on the federal terrorist watchlist.

48. Additionally, the federal government utilizes automated algorithms and risk-based targeting rules to select individuals for scrutiny, investigation, and nomination to one or more terrorist watchlists.

49. In order to designate a person on the federal terrorist watchlist, a federal government official, including a CBP officer, must make a nomination in accordance with the established nomination policies and procedures described above, and a TSC official must accept the nomination. TSC officials accept nominations at a rate above 98 percent.

50. Based on the facts alleged in this Complaint and the publicly known processes of the federal terrorist watchlist, a quantitative analysis can be constructed to measure and describe the performance and efficacy of the federal terrorist watchlist.

51. A quantitative analysis requires that, in order to accomplish the federal terrorist watchlist's stated objectives, Defendants must have at least some greater-than-random

abilities to identify future terrorists. This is due to the nature of the processes the federal government utilizes to place persons on the federal terrorist watchlist and the size of the population Defendants can—if they so choose—screen against the federal terrorist watchlist's inclusion standards.

52. A quantitative analysis demonstrates that the federal government's watchlisting system would perform similarly if inclusion on the watchlist was done via random selection instead of the existing inclusion standards it utilizes.

53. A quantitative analysis indicates that the federal government has no ability to watchlist persons whose placement on the watchlist would further the federal government's—or CBP's—stated objectives.

CBP Policies Violate the Constitutional Rights of TSDB Listees

54. Anyone listed in the TSDB is subjected to varying forms of heightened scrutiny and adverse repercussions by CBP.

55. The "information in [the] TSDB [contains] merely the identifying information of the person entered into the TSDB, and does not include the "derogatory information," or "totality of the circumstances," that is the basis of a nomination by the FBI."

56. As such, TSDB information shared with CBP also contains merely the identifying information of TSDB listee and does not include the "derogatory information," or "totality of the circumstances," that formed the basis of a nomination by the FBI.

57. Although CBP has access to TSDB information provided by the TSC, it is the TSC that maintains and controls the TSDB database.

58. CBP automatically designates TSDB listees as "Armed and Dangerous," refers them to secondary inspection, and otherwise automatically flags them as potential terrorists in automated alerts sent to officers.

59. All travelers, including Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals, that present themselves at a port of entry, whether at a land border crossing or an airport, interact with officers from CBP for entry into the United States and are queried by CBP against TECS, a CBP system that includes TSDB information shared by the Terrorist Screening Center "seamlessly and in realtime."

60. Airlines are required to provide a complete passenger manifest to CBP before a flight can depart or enter the United States and CBP queries the identities of all passengers on those manifests against the Advance Passenger Information System ("APIS"), an automated targeting system that feeds biographical information of passengers into TECS.

61. CBP can also conduct additional screening and questioning of individual airline passengers prior to departing the United States if a passenger matches TSDB information in TECS.

62. As a matter of policy and practice, CBP primary inspection officers are alerted that TSDB listees are a "potential match" to TSDB in TECS and refer them to secondary inspection for questioning to determine if the traveler is in fact a "potential match."

63. CBP officers do not have access to the underlying derogatory information that formed the basis for a traveler being listed in the TSDB.

64. CBP Officers conducting the secondary inspection are directed to contact the National Targeting Center ("NTC"), a division within CBP Field Operations that works with the TSC, which ultimately makes a final determination on whether the traveler is a match to the TSDB.

65. CBP records in TECS a summary of the secondary inspection that includes whether a determination was made by NTC as to whether the traveler was confirmed to be a match.

66. Despite having gone through this TSDB matching process during secondary inspection, each time a traveler who was previously confirmed as a match to the TSDB presents themselves for inspection at a port of entry, CBP primary inspection officers receive the same alert that the traveler is a "potential match" because they do not have access to or knowledge of previous inspections, and accordingly the TSDB listee is referred back to secondary inspection to go through the TSDB match process all over again.

67. Even if CBP determines a traveler is not a match to the TSDB and records that information in TECS, unless the TSC updates the TSDB, the next time that traveler presents themselves at a port of entry for inspection, the CBP primary inspection officer will receive the same alert that the traveler is a "potential match" to the TSDB and will refer that traveler to secondary inspection to undergo the TSDB match process all over again.

68. Pursuant to official CBP policy, CBP officers refer TSDB listees to secondary inspection and the TSDB listees are compelled as a matter of process to provide biometric fingerprints to determine whether they are a match to the TSDB.

69. Pursuant to official CBP policy, CBP officers may handcuff TSDB listees before referring them to secondary inspection.

70. Pursuant to official CBP policy issued in 2018, CBP officers are directed to conduct an advanced forensic search of any electronics carried by TSDB listees:

> An advanced search is any search in which an officer connects external equipment through a wired or wireless connection to an electronic device not merely to gain access to the device, but to review, copy, and analyze its contents.[2]

71. "The presence of an individual on a government operated and government vetted terrorist watch list," alone constitutes grounds for the CBP to search, copy, store, and analyze the contents of laptops, tablets, and smartphones, etc. without requesting or obtaining consent. (Hereinafter the "CBP electronic devices policy").

72. Pursuant to the CBP electronic devices policy, CBP officers are directed to disregard factors for and against a search and seizure of electronic devices in the possession of TSDB listees and to conduct a nonroutine forensic search and seizure of all electronics despite not having access to the underlying derogatory information that formed the basis of the TSDB listees' nomination to the TSDB.

73. CBP officers seize, search, download, copy, analyze, and conduct a forensic search of the contents of the electronic devices, including those of each of the Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals.

74. The prior version of the CBP electronic devices policy adopted in 2008 similarly directed CBP officers to copy data off of the electronic devices of TSDB listees, and it was and continues to be standard practice to do so and outside the view of the TSDB listee.

Abdulkadir Nur

75. Plaintiff Abdulkadir Nur is a prominent business owner and humanitarian, and as part of his employment, frequently travels both internationally and within the U.S.

[2] *See* CBP Directive No. 3340-049A (January 2018).

76. Mr. Nur is also the CEO of a water welling and drilling company in Somalia and has worked with humanitarian groups such as the Red Cross since 1997 delivering food and resources to impoverished communities in East Africa.

77. In September 2008, while providing logistical support to a United Nations relief program, delivering food and other aid in areas of Somalia devastated by conflict, Mr. Nur's caravan was raided by local insurgents. A United Nations Monitor Group subsequently launched an investigation, with which Mr. Nur participated fully, that ultimately found no fault in Mr. Nur's actions.

78. This investigation, however, drew the attention of the FBI and U.S. Attorney's Office, who demanded financial records and data from Mr. Nur and his company. Mr. Nur complied fully and provided everything requested, only interested in maintaining his good name and reputation.

79. In 2009, shortly after the UN Monitor Group report was released, the FBI and U.S. Attorney's Office told Mr. Nur they were no longer interested in bringing charges, and they stopped returning his calls to provide further exculpatory evidence.

80. Since around that time, however, Mr. Nur has been the target of increased scrutiny at airports and border crossings, consistently noticing "SSSS" on his boarding pass, always being subjected to secondary inspection and interrogation—all telltale signs that the government had assigned him a disfavored status that would subject him to a segregated process in all of his encounters with the federal government.

81. Mr. Nur did not travel to the United States for several years between approximately 2010 and 2018.

82. In 2018, the Government's targeting of Mr. Nur at airports and border crossings ramped up to include unreasonable search and seizure, both of his person and his electronic

devices, enhanced screening, hours-long delays, prolonged interrogations including harassing, aggressive behavior, and detention in separate interrogation rooms, not to mention flight delays and cancellations.

83. Following every flight into the United States since 2018, Unknown CBP Officers have seized Mr. Nur's electronic devices, demanding the passwords. Believing he had no choice but to comply and afraid his refusal would prolong his detention, Mr. Nur gave the passwords, including biometric scans, to the officers who took those devices out of the room, to copy, download, or upload data, and then returned them upon Mr. Nur's eventual release.

84. Since 2020, however, Mr. Nur began refusing to give officers the passwords to his devices. In some instances, this refusal was met by aggressive intimidation tactics. Officers still took the devices out of the room, and on multiple occasions, seized them completely, refusing to return them until an extended, forensicsearch could be conducted offsite days or weeks later.

85. On or about April 28, 2018, Mr. Nur flew from Toronto to Boston. He was taken by American CBP officers into a separate interrogation room where officers probed his occupation, family relationships, and religion. During and after the interrogation, officers took his electronic devices into another room after asking for and receiving the passwords. Mr. Nur was detained more than five hours and missed his connecting flight.

86. On or about October 9, 2019, Mr. Nur flew from Dubai to Dulles International Airport and received similar treatment. He was detained in a separate interrogation room for several hours, aggressively patted down, searched, and interrogated regarding his work, family, and religion. After demanding his passwords, officers took Mr. Nur's electronic devices out of the room, upon information and belief, to be searched and data copied, uploaded, or downloaded.

87. In or about February 2020, Mr. Nur again flew into Dulles International Airport, and again was subjected to detention in a separate interrogation room for several hours, enhanced search, interrogation, and demand for his passwords to search his electronic devices, which he gave. The devices were again removed from his sight, on information and belief, data to be copied, downloaded, or uploaded.

88. On or about June 30, 2020, Mr. Nur boarded a flight from Dar es Salaam to Dulles International Airport after five days of being denied boarding at two different airports by U.S. officials. Mr. Nur originally planned to return to Washington, D.C. from Nairobi via Addis Ababa on June 25 but was denied a boarding pass because "the U.S. government had not cleared him in the system" to travel to the U.S. After contacting the U.S. Embassy, Mr. Nur was assured he would be able to board the next day, but the problem persisted. So he drove 18 hours to Dar es Salaam hoping for a better result. Again, he was turned away from two booked flights at the hands of the U.S. government before finally being allowed to board on June 30.

89. Upon arrival at Dulles International Airport, Mr. Nur was again escorted to an interrogation room and detained for several hours while being searched, patted down, and interrogated. This time, when officers asked for the passwords to his electronic devices, Mr. Nur refused. He was shoved against the wall and aggressively searched, deprived of his shoes, intimidated, and threatened by officers. When he continued to refuse, officers eventually released him and his devices.

90. On or about August 15, 2020, Mr. Nur again flew from Dubai to Dulles International Airport, where officers detained him in a separate interrogation room while they continued to search, inspect, interrogate, and demand his electronics passwords. When he refused, officers again became aggressive in an attempt to intimidate Mr. Nur into acquiescing. When

that did not work, officers took his devices into another room, and an agent believed to be FBI – though the agent refused to identify himself – interrogated him further.

91. On or about May 4, 2021, Mr. Nur flew from Dubai to Boston and was again detained in a separate interrogation room, searched aggressively, interrogated, and his passwords demanded. When he refused to deliver passwords or answer questions, the officers took his devices and held him for several hours.

92. In or about September 2021, Mr. Nur again flew into Dulles airport. CBP officers were waiting at the customs queue when he arrived. Before interrogation could begin, Mr. Nur produced a letter from his attorney instructing CBP that he was represented and would not submit to questioning. Officers retrieved his luggage, opened them on the table, and kept his passport while he was led into a separate interrogation room. One agent questioned him regarding his business, family, history with CBP and electronic devices. Mr. Nur refused to answer. Officers searched his luggage, jacket, wallet, pockets aggressively several times, emptying everything. When Mr. Nur commented that this is a waste of resources, the officer made clear that he was just doing his job and that the mandate to search in this manner came from the system and not the reasonable judgment any CBP agent. Because he refused to give officers his electronics passwords, they seized a laptop computer, cell phone, and flash drive, which were then shipped to his lawyers' office two weeks later.

93. On or about January 25, 2022, Mr. Nur flew into Washington Dulles Airport from Nairobi, Kenya via Addis Ababa. Upon arrival in the U.S., an agent came directly to him, in the middle of the Customs line, and led him to a separate interrogation room where he was detained, his luggage searched out of his sight, and his devices taken. When he refused to give the agent the passwords to the devices, the agent promised the detention would be over quicker if Mr. Nur complied. When that tactic did not work, the agent insisted, threatening to

keep the devices if he did not hand over the passwords. Mr. Nur again refused and told the agent he wanted his lawyer present for any interrogation. Mr. Nur refused to answer any questions and was held for nearly two hours.

94. Mr. Nur minimizes his travel as much as possible in order to avoid the intense fear and expense that come with being labeled by the U.S. Government as a "known or suspected terrorist" because of his status on the Government's federal terrorist watchlist.

95. Upon information and belief, Mr. Nur's family members that travel with him are subjected to the above-described treatment because of their relation to him and because of his status on Defendant's federal terrorist watchlist.

96. Upon information and belief, Mr. Nur still remains on the federal terrorist watchlist.

COUNT I
VIOLATION OF THE FOURTH AMENDMENT
TO THE UNITED STATES CONSTITUTION (Electronic Search and Seizure)
(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)
(Against Official Capacity Defendants only)

97. The foregoing allegations are realleged and incorporated herein.

98. Plaintiff and similarly situated Americans have the right "to be secure in their… papers… against unreasonable searches and seizures." Const. amend. IV.

99. As a matter of official policy and practice, Defendant refers TSDB listees to secondary inspection where they are compelled as a matter of process to provide biometric fingerprints to determine whether the TSDB listee is a match to the TSDB.

100. As a matter of official policy and practice, Defendants seize, search, download, copy, analyze, and conduct a forensic search of the contents of the electronic devices of individuals on the TSDB when presenting themselves at the border or at the airport, including Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals.

Defendants routinely do not return the electronic devices to the watchlisted individuals for weeks or months, if not longer. See CBP Directive No. 3340-049A.

101. As a matter of official policy and practice, and particularly at the border, Defendants download and copy the contents of watchlisted individuals' electronic devices, including those of Plaintiff, onto Defendant's computers and upload those contents to Defendant's watchlisting and intelligence databases. Defendants then review that material in a manner which constitutes a search for Fourth Amendment and other purposes.

102. As a matter of official policy and practice, Defendants utilize the contents of watchlisted individuals' electronic devices, including those of Plaintiff, as a source of intelligence. Defendants also utilize the contents and contacts of watchlisted individuals' electronic devices, including those of Plaintiff, to launch investigations into and nominate associates of the watchlisted individual for rules-based terrorist monitoring and inclusion in the federal terrorist watchlist.

103. Defendants, after seizing Plaintiff's electronic devices, have forced him to open those devices, including by providing passwords and by using biometric means such as facial recognition or fingerprints.

104. Defendants' demands were not mere requests and given the circumstance of the demand (including the ongoing seizure of Plaintiff) and the consequences often expressed by CBP officers regarding noncompliance (lengthy and indefinite detention and potentially permanent confiscation of the device), no reasonable person in Plaintiff's position would take Defendants' demands to be a mere request.

105. Even if demands for passwords and biometric data are permissible under the Fifth Amendment, they result in an intrusion of privacy that is the equivalent of a forensic search under the Fourth Amendment.

106. CBP policy permits and generally performs searches (including forensic searches) and seizures of electronics solely on the basis of watchlist placement.

107. Watchlist placement does not satisfy any probable cause standard.

108. Watchlist status does not satisfy a reasonable suspicion of a border-related crime or inadmissibility because (1) it is not an actual reasonable suspicion standard, (2) it does not require reasonable suspicion of any crime, (3) it does not require reasonable suspicion of any border related crime, (4) it does not require reasonable suspicion that there is anything in Plaintiff's electronic devices that is related to any border-related issue, and (5) it does not require reasonable suspicion there is any contraband in Plaintiff's electronic devices.

109. Defendants confiscated Plaintiff's electronic devices, copied the devices' contents, and searched and utilized those contents for intelligence and investigations that are not related to any border-related crime, and generally are not related to any particular crime at all.

110. Defendants engaged in these seizures and searches solely because Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals are listed on the federal terrorist watchlist.

111. Defendants violated the rights of Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals listed on the federal terrorist watchlist to be free from unreasonable search and seizure under the Fourth Amendment to the United States Constitution and their reasonable expectations of privacy when they confiscated Plaintiff's electronic devices, copied the devices' contents, and searched and utilized those contents for intelligence and investigations that are not related to any border-related crime.

112. Defendants's forensic searches of Plaintiff's electronic devices and the electronic devices of similarly-situated American citizens, permanent residents, and foreign nationals are nonroutine border searches that required and were not based on individualized suspicion in

violation of their Fourth Amendment rights. *U.S. v. Montoya de Hernandez*, 473 U.S. 531, 538, 540-41 & n.4 (1985); *United States v. Kolsuz*, 890 F.3d 133, 144 (4th Cir. 2018), as amended (May 18, 2018); *U.S. v. Cotterman*, 709 F.3d 952, 963–68 (holding that forensic examination of computer is nonroutine border search requiring reasonable suspicion); *U.S. v. Saboonchi*, *United States v. Saboonchi*, 990 F. Supp. 2d 536, 548 (D. Md. 2014) (same as to smartphones and flash drives).

113. Defendants' forensic searches of Plaintiff's electronic devices and the electronic devices of similarly-situated American citizens, permanent residents, and foreign nationals are not subject to the border search exception because there is no direct link between the search of Plaintiff's electronic devices and the electronic devices of similarly situated Americans and any government interest that justified the searches on any account of a nexus requirement in violation of their Fourth Amendment rights. *United States v. Kolsuz*, 890 F.3d 133, 143 (4th Cir. 2018), as amended (May 18, 2018).

114. Defendant CBP's policy that the presence of an individual on a "government operated and government vetted terrorist watch list" alone constitutes grounds for CBP officers to search, copy, store and analyze the contents of laptops, tablets, and smartphones, without any individualized suspicion of the particular Plaintiff or similarly situated American citizens, permanent residents, and foreign nationals being stopped is a violation of their Fourth Amendment rights.

115. Defendants' policies requiring CBP officers and TSA agents to disregard "all the facts surrounding the traveler and [their] trip" and "factors for and against reasonable suspicion," and to conduct a nonroutine forensic search of Plaintiff's electronic devices and the electronic devices of similarly situated American citizens, permanent residents, and foreign nationals based upon the mere presence of identifying information without derogatory

information that formed the basis of the TSDB nomination violates their rights under Fourth Amendment. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541 (1985); *Manzo–Jurado*, 457 F.3d 928 (9th Cir. at 938) (the reasonable suspicion determination must "take[ ] into account both factors weighing for and against reasonable suspicion.")

116. Because the TSDB includes tens of thousands of innocent travelers and is "based on broad profiles which cast suspicion on entire categories of people without any individualized suspicion of the particular person to be stopped," Defendants violated the Fourth Amendment rights of Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals when they confiscated their electronic devices, copied the devices' contents, and searched and utilized those contents for intelligence and investigations that are not related to any border-related crime. See *Reid v. Georgia*, 448 U.S. 438, 441 (1980); *United States v. Sigmond–Ballesteros*, 285 F.3d 1117, 1121 (9th Cir.2001) (internal quotations and citations omitted).

117. Defendants lacked consent, reasonable suspicion, probable cause, or a warrant for the seizures and searches of Plaintiff's electronic devices and the electronic devices of similarly situated American citizens, permanent residents, and foreign nationals when they confiscated their electronic devices, copied the devices' contents, and searched and utilized those contents for intelligence and investigations that are not related to any border-related crime. *See United States v. Kolsuz,* 185 F. Supp. 3d 843, 853 (E.D. Va. 2016), *aff'd*, 890 F.3d 133 (4th Cir. 2018), *as amended* (May 18, 2018).

118. Defendants knew at the time that they confiscated the electronic devices of Plaintiff and the electronic devices of similarly situated American citizens, permanent residents, and foreign nationals, copied the devices' contents, and searched and utilized those contents for intelligence and investigations that are not related to any border-related crime Plaintiff's

electronic devices and the electronic devices of similarly situated Americans when they presented themselves at the border and at the airport that they were violating their reasonable expectations of privacy and their rights to be free from unreasonable search and seizure under the Fourth Amendment to the United States Constitution.

119. By placing Plaintiff and similarly situated American citizens, permanent residents, and foreign nationals on the federal terrorist watchlist, Defendants have caused him an actual, imminent, and irreparable injury that cannot be undone through monetary remedies.

WHEREFORE, Plaintiff request this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

COUNT II
VIOLATION OF THE FIFTH AMENDMENT
TO THE UNITED STATES CONSTITUTION (Self-Incrimination)
(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)
(Against Official Capacity Defendants only)

120. The foregoing allegations are realleged and incorporated herein.

121. The Fifth Amendment protects the fundamental individual right against self-incrimination. U.S. Const. amend. V.

122. The Fifth Amendment protects every person from incrimination by the use of evidence obtained through search or seizure made in violation of his or her rights under the Fourth Amendment. *Agnello v. United States*, 269 U.S. 20, 33–34 (1925).

123. As a matter of official policy and practice, Defendant refers TSDB listees to secondary inspection where they are compelled as a matter of process to provide biometric fingerprints to determine whether the TSDB listee is a match to the TSDB.

124. Defendants, after seizing Plaintiff's electronic devices, have forced him to open those devices, including by providing passwords and by using biometric means such as facial recognition or fingerprints.

125. Defendant's demands were not mere requests, and given the circumstance of the demand (including the ongoing seizure of Plaintiff) and the consequences often expressed by CBP officers regarding noncompliance (lengthy and indefinite detention and potentially permanent confiscation of the device), no reasonable person in Plaintiff's position would take Defendant's demands to be a mere request.

126. Even if the Government had the right to seize and search a device, that does not allow the Government to infringe upon an individual's other rights.

127. Requiring the providing of passwords or the use of biometric means such as facial recognition or fingerprints violates the Fifth Amendment.

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

COUNT III
VIOLATION OF THE ADMINISTRATIVE PROCEDURE ACT
(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)
(Against Official Capacity Defendants only)

128. The foregoing allegations are realleged and incorporated herein.

129. For the reasons explained in Counts I-III, Defendant's policies of searching and seizing Plaintiff and other United States citizens and permanent residents on the federal watchlist, as well as searching and seizing their cell phones, are arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and contrary to constitutional rights, power, privilege, or immunity, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

130. Even if constitutional, Defendants' policies of permitting seizure and forensic searches of watchlisted individuals solely based on watchlist status are arbitrary and capricious, an abuse of discretion, and otherwise not in accordance with law, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

131. Even if constitutional, Defendants' policies of seizing individuals and their devices at the border and ordering them to provide passwords and biometric data, including by suggesting that failure would lead to prolonged detention, confiscation or seizure of the person or the electronic device, are arbitrary and capricious, an abuse of discretion, and otherwise not in accordance with law, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

132. Even if constitutional, Defendants' policies of seizing and detaining watchlisted individuals for hours in order to perform a non-border-related interrogation of those individuals are arbitrary and capricious, an abuse of discretion, and otherwise not in accordance with law, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

COUNT IV
VIOLATION OF THE FOURTH AND FIFTH AMENDMENTS TO THE UNITED STATES CONSTITUTION (*Bivens*)
(Jurisdiction under 28 U.S.C. § 1331, *Bivens v. Six Unnamed Agents* and 5 U.S.C. § 702)
(Against Unknown CBP Officers only)

133. The foregoing allegations are realleged and incorporated herein.

134. As explained in Counts I and II, the CBP has violated Plaintiff's rights under the Fourth and Fifth Amendment.

135. The Defendant CBP Officers were the specific individuals who carried out these

constitutional injuries.

136. Because of the violations described in Count I and II executed by the Defendant CBP Officers, and particularly the search and seizure of his electronic devices, Mr. Nur experiences a substantial violation of his sense of privacy knowing that federal officials are harvesting his personal conversations with loved ones, his humanitarian work in Somalia, and even his sensitive medical information. His personal and professional lives are reflected in the data on Mr. Nur's electronic devices, and the privacy violation inflicted when that data is taken from him causes fear, a loss of dignity, and deters him from traveling to the United States.

137. Defendant CBP Officers knew or should have known that their searching and seizures of Mr. Nur's devices, as well as their demands that he provide passwords and biometric data, violated Mr. Nur's clearly established constitutional rights.

WHEREFORE, Plaintiff requests this Honorable Court grant damages to Mr. Nur against the Defendant CBP Officers in an amount to be proved at trial, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

Prayer for Relief

WHEREFORE, Plaintiff respectfully request against the Official Capacity Defendants:

138. A declaratory judgment that Defendant's policies, practices, and customs violate the Fourth and Fifth Amendment to the United States Constitution and the Administrative Procedure Act.

139. A declaratory judgment that Defendants require reasonable suspicion of a border related crime, contraband, or inadmissibility, apart from watchlist status, before

performing a nonroutine search or seizure of persons on the watchlist or forensic searches of their electronic devices.

140. A declaratory judgment that Defendants placed Mr. Nur on the watchlist illegally and unlawfully imposed consequences tied to that status.

141. An injunction that:

a. Prohibits Defendants from applying CBP Policy that permits a forensic search of the electronic devices of US citizens or permanent residents solely because of watchlist status.

b. Prohibits Defendants from applying CBP Policy that permits nonroutine detention and interrogation of US citizens or permanent residents solely because of watchlist status.

c. Prohibits Defendants from ordering individuals at the border provide passwords or biometric means to access electronic devices, including by asserting or suggesting consequences (such as prolonged detention, confiscation or seizure of the person or the electronic device) for failure to provide passwords or biometric means of access.

d. Ordering Defendants to remove the status and annotations imposed on Mr. Nur, expunge any records regarding his illegal status and annotations, and expunge any information illegally seized from Mr. Nur and

142. An award of attorneys' fees, costs, and expenses of all litigation, pursuant to 28

U.S.C. § 2412; and,

143. Such other and further relief as the Court may deem just and proper.

WHEREFORE, Plaintiff requests this Honorable Court grant damages to Mr. Nur

against the Defendant CBP Officers in an amount to be proved at trial, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

JURY DEMAND

NOW COME Plaintiff, by and through their undersigned counsel, and hereby demand trial by jury of the above-referenced causes of action.

Dated: February 11, 2022

Respectfully submitted,

CAIR LEGAL DEFENSE FUND
BY: /s/ Lena F. Masri
Lena F. Masri (VA 93291
lmasri@cair.com
Gadeir I. Abbas (VA 81161)*
gabbas@cair.com
Justin Sadowsky (VA 73382)
jsadowsky@cair.com
Kimberly Noe-Lehenbauer (OK 34744)[+^]
knoelehenbauer@cair.com
453 New Jersey Ave., S.E.
Washington, DC 20003
Phone: (202) 742-6420
Fax: (202) 488-0833

**Mr. Abbas licensed in VA, not in D.C. Practice limited to federal matters.*

[+]Ms. Noe-Lehenbauer licensed in OK, not in D.C. Practice limited to federal matters.

^Application pro hac vice forthcoming.

Attorneys for Plaintiff